

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
3 July 2003 (03.07.2003)

PCT

(10) International Publication Number
WO 03/055170 A1(51) International Patent Classification⁷: H04L 29/06

(21) International Application Number: PCT/EP02/13493

(22) International Filing Date:
29 November 2002 (29.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
01130600.8 21 December 2001 (21.12.2001) EP

(71) Applicant (for all designated States except US): INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant (for LU only): IBM DEUTSCHLAND GMBH [DE/DE]; Pascalstrasse 100, 70569 Stuttgart (DE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): ARNOLD, Ok-sana [DE/DE]; Flughafenstr. 6d, 60528 Frankfurt (DE).

WERNER, Andreas [DE/DE]; Am Pfingstborn 10, 61479 Glashuetten (DE). KRAEMER, Ulrich [DE/DE]; Frankfurter Strasse 76, 64293 Darmstadt (DE). LENTZ, Thomas [DE/DE]; Homburgerstr. 10, 60486 Frankfurt/M (DE).

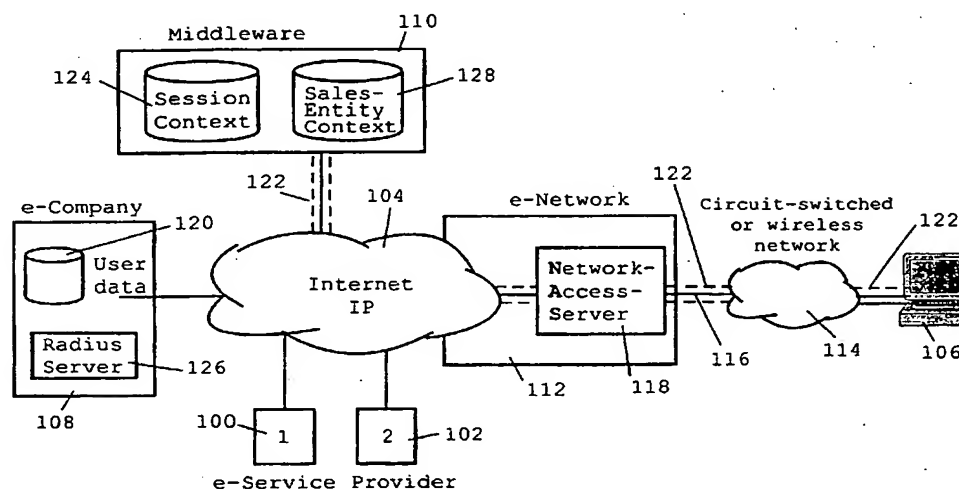
(74) Agent: KAUFFMANN, Wolfgang; IBM Deutschland GmbH, Intellectual Property, 70548 Stuttgart (DE).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR SECURE HANDLING OF ELECTRONIC BUSINESS TRANSACTIONS ON THE INTERNET



(57) Abstract: Disclosed is a computer-based technology for handling end-to-end business transactions in a TCP/IP-environment. A managing instance enables logon and provides a pool of IP addresses available for allocation. The managing instance allocates an IP address from the pool and establishes a tunneling IP connection between the managing instance and a user's device. The user's IP address together with any attributes relevant for accounting, authentication and authorization (AAA) are stored during the session time. The correlation between a user's authentication name and an IP address assigned to that name as well as the book-keeping of the validity of that correlation is handled using a session context. Any identification process for a user/subscriber who would like to use any service offered by an e-Service provider will be conducted solely using the assigned IP address.

WO 03/055170 A1



TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

- 1 -

D E S C R I P T I O N

METHOD AND SYSTEM FOR SECURE HANDLING OF ELECTRONIC BUSINESS
TRANSACTIONS ON THE INTERNET

BACKGROUND OF THE INVENTION

The invention generally is in the field of computer-related transactions in the Internet arena and more specifically concerns a method and system for handling end-to-end business transactions in a Transmission Control Protocol/Internet Protocol (TCP/IP) environment.

Known Business-to-Customer (B2C) or Business-to-Business (B2B) service transactions can be divided into services being delivered electronically, e.g. media streaming, file transfer, e-mail, SMS, games, etc., and services which demand for physical delivery of goods like retail business. Professional websites or web portals providing the aforementioned services need to have implemented a process for limiting user access to those users having necessary access rights.

A known particular problem in that arena thus is authentication by third parties, in the following simply referred to as user authentication. Since the Internet Protocol, under a process view, is stateless, in order to guarantee authenticity of a user entering an access restricted website or web portal, it is necessary to perform a user authentication procedure repeatedly when entering another or even the same website or portal again.

- 2 -

A first approach addressing the above issue is disclosed in European patent application EP 1 039 724 A2. Described is a system for user authentication by means of the user's IP address which is assigned to a user's computer by a Dynamic Host Configuration Protocol (DHCP) server. Hereby the data pair user/IP address is used for user authentication on side of an authentication server. After that server has detected that the user is authorized, the mentioned data pair is stored in a Lightweight Directory Access Protocol (LDAP) server. The stored information can then be used for authentication of the user in applications running on other computers.

As another approach, PCT application WO 113 598 A2 discloses a dynamic wireless Internet address assignment scheme for user authentication. A unique IP address is assigned to a user of a mobile communication device communicating via an Optical Burst-Switching (OBS) network. The OBS, in particular, includes a master ticketing authority that maintains a database of unique IP addresses that can be assigned to users entering the network. The OBS further includes a gateway, a master routing database, and at least one mobile communication device in contact with an OBS. In that approach, authentication of users in the network is accomplished through the transmittal of encrypted random numbers between a user authentication site and a mobile communication device.

The above discussed prior art approaches comprise or require rather complex and expensive technology for handling the subject end-to-end business transactions between a user and one or more Internet sales-entity (product, etc.) and/or service providers where the business transaction strictly requires access authorization by the user to the one or more websites or -portals.

- 3 -

In addition, the above mentioned DHCP protocol does not allow to determine the end or termination of an existing online session of a user. Since an IP address is allocated dynamically, a third person can principally abuse an already allocated IP address, as the IP address is still registered on the LDAP server in the name of the preceding user. This existing approach insofar can not be regarded to be secure.

In addition, the known approaches do not provide a technically simplified platform for service delivery and payment in an IP environment on the Internet, as mentioned beforehand. In addition, accounting within the internet is not solved at the moment in general. Furthermore, there is no network based on the edge available authentication and access control facility. Nowadays every service provider has to install their own application specific solution.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method and system for handling beforehand discussed end-to-end business transactions, i.e. transactions between a user and a sales-entity/service provider as defined above but not e.g. transactions between a user and an Internet Service Provider (ISP), which enable a secure way related predominantly to determination and/or trust of authenticity of both persons involved in the transaction and which enable to perform those business transactions with minimum technical and cost efforts.

- 4 -

The above objects are achieved by the features of the independent claims. Advantageous embodiments are subject matter of the subclaims.

The underlying concept of the invention is provision of a managing or server instance, preferably being implemented as a middleware arranged between an IP layer and a server layer in the known Open Systems Interconnection (OSI) reference model, that allows for a one time and unique user or subscriber logon, hereinafter referred to as "single sign-on" (SSO) and that provides a pool of IP addresses available for allocation to such users. With the approval of the user logon, the server instance allocates an IP address from the pool and a continuous point-to-point (PPP) IP connection between the server instance and the user's computer or telecommunication device is established. At the same time, the user's IP address together with any attributes relevant for accounting, authentication and authorization (AAA) are recorded or stored. Further, the user's network access is continuously monitored and it is determined if said online session is terminated. If so, the allocated IP address for the user is invalidated and said IP address provided back to said pool of IP addresses.

In a preferred embodiment, a tunneling IP connection (virtual private network connection) is continuously established between the server instance and a user's computer or telecommunication device wherein providing a very reliable mechanism for detection of the termination of an online session by a user thus securely prevents the above mentioned situation with increased potential of abuse or misuse of an already assigned IP address. It should be emphasized that reliability of that mechanism is mainly obtained through the

- 5 -

combination of the continuous IP connection and the direct monitoring of the user's network access behavior.

In one aspect of the invention, the user's current IP address is used as an authorization token during the following online session. Now, the stored information can be made available by the server instance to an e-Company where the particular user/subscriber has a valid subscription, standard protocols to IP applications for authentication, authorization, and accounting can be applied between the e-Company and any e-Service provider with whom the user/subscriber is interested to conduct any kind of e-Commerce business(es).

In another aspect, at least said IP address allocated to said user together with at least one attribute relevant for accounting and/or authentication and/or authorization are continuously recorded or being stored. An exemplary attribute is the user's telephone number.

In another aspect, the server instance (middleware) keeps full control of the IP address assignment process in view of the limited pool of available IP addresses and the role of the server instance for assigning an IP address to a signed-on user and thus the IP address, in accordance with the invention, functions as a unique identifier for a user that can be used for further authentication procedures to be conducted during the following online session by the user.

In accordance with the proposed authentication process, an IP address is assigned to the user/subscriber during the single sign-on authentication procedure performed in the network of the respectively underlying network service provider of the user or the like. It is emphasized hereby that assignment or

- 6 -

allocation of the IP address from the pool of available IP addresses is a necessary part of the proposed functionality of the server instance or middleware, respectively. The proposed procedure hereby supports assignment of dynamic IP addresses as well as static IP addresses.

The correlation between a user's authentication name and the existing IP address assigned to that name as well as the book-keeping of the validity of that correlation is handled exclusively by the above mentioned server instance (middleware) by means of a session context. Any identification process for a user/subscriber who would like to use any service offered by an e-Service provider will be conducted solely using the assigned IP address. As a consequence, the real identity e.g. represented by the user name or other user specific information, must not necessarily be provided to the above mentioned e-Service provider(s). However, certain user attributes, if additionally required for requested services and/or goods, can exceptionally be made available to the e-Service provider(s) by the middleware. For the latter procedure only the IP address assigned to the user/subscriber at the time of provision of such additional information is required.

In a preferred embodiment, the session context comprises or includes transaction events performed by the user, in particular accounting starts or the like in order to continuously keep valid authenticity of the user during a whole online session and in order to use the existing authorization by the user end-to-end business transactions like video-on-demand services offered on websites or Internet portals of e-Service providers.

- 7 -

The proposed mechanism thus advantageously allows a user to approach different commercial websites or portals on the Internet during a continuing online session in order to perform different B2C transactions as mentioned above. For handling those transactions, the user is not required to conduct further sign-on procedures on side of the e-Service providers again and again since the server instance keeps an existing measure for authenticity of the user. Further, AAA procedures are handled by only one instance, namely the server instance according to the invention. The invention hence is a general solution to the problem of reliable Authentication, Authorization, and Accounting regardless of the technology and method to access the IP services.

When the user signs (logs) out or is somehow disconnected from the server instance, the server instance terminates the user's session context and by this closes the currently pending user session. After that all provisioned services will be stopped and no authorization will be granted, until the user logs in again. However, any pending sales entity context beyond the will continue independently of the terminated session context. The information within the database will be used to provide the connection between services, to be provisioned and accounted, and the user or subscriber account. The accounting information too will be available for any billing application associated with the service or the access provider. The proposed session context therefore solves the above mentioned problem of statelessness of TCP/IP, too.

It is noteworthy that the combination of single registry (SSO) and processing of a user's IP address in order to obtain an uninterrupted session context which is continuously maintained during the following user session guarantees authenticity of

- 8 -

the user throughout the continuous online session and thus it is advantageously avoided to perform further sign-on procedures on side of each sales-entity and/or service provider approached during the session.

In other words, the IP address is used by the invention as a key instrument of the proposed server instance since the IP address is the only information required for any service instance in any of the two groups (virtual/real) to resolve an authorization request towards the server instance. This is the base for secure charging or payment, Quality-of-Service (QoS) delivery and consumption. Another advantage of this technique is that the client is anonymous outside, on any service layer. Potentially any real world entity represented by an IP-address may become a service recipient which may require billing.

The proposed process enables securely handling of the above mentioned transactions, despite the pre-mentioned statelessness of TCP/IP protocol, and thus effectively prevents the sales-entity and/or service providers from intrusions by others, i.e. non-authorized accesses to access-restricted websites or Internet portals, due to the session context related access control based on the unique IP address. The randomly changing IP address between consecutive sessions guarantees maximum secure access authorization handling. The invention thus effectively protects sales-entity and/or service providers against illegal intrusions by unauthorized users but with minimum security efforts. It is further to be noted that the session context, due to its randomized character, can not be simulated by an intruder. In addition, delivery and payment are solved in any conceivable scenario using the Internet Communication Protocol TCP/IP as basic transport scheme for e-companies integration. Thereupon, no

- 9 -

additional information has to be transferred in order to conduct further sign-on procedures by the user during the session.

The invention can be applied to computer networks on a global scale. The only requirement is that the users have some IP connectivity. The proposed server instance, in a first aspect, can be part of a global network like IBM's global network or any other messaging service network (MSN). This would yield a business model comprising only one player as payment mediator controlling any business transaction between customers and service providers on the one hand, and sell and charge his own services directly to his users/subscribers on the other hand.

Alternatively, the server instance can be provided by a large network operator, e.g. a common application service provider (ASP) or telecommunication company which will provide hosting services to any number of e-companies. In this case either that company offers payment mediation services, or any hosted e-company, or both.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in the following by way of a preferred embodiment. Hereby reference is made to the accompanying drawings. In the drawings

Fig. 1 is an overview block diagram illustrating a typical B2C service Internet environment in accordance with the invention;

- 10 -

Fig. 2 illustrates basic principles for assignment of IP addresses on the Internet according to the prior art;

Fig. 3 depicts the process flow of a preferred embodiment of the invention by way of a flow diagram;

Fig. 4 illustrates the RADIUS protocol known in the prior art for providing authentication, authorization and configuration information between a Network Access Server (NAS) and a Shared Authentication Server;

Fig. 5 is a schematic block diagram illustrating a network layer structure including a middleware according to the invention;

Fig. 6 illustrates interoperation of the proposed middleware with a number of e-Companies; and

Fig. 7 depicts possible integration profiles for the main components of the network layer structure shown in Fig. 5.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The B2C environment exemplarily shown in Fig. 1 illustrates the basic principals of the invention by way of a typical B2C Internet environment including two exemplary (Internet) e-Service providers 100, 102 (in the following referred to as 'sales-entity or service providers') connected to the Internet 104 which stand for a number of other potential sales-entity/service providers not shown here. The shown network environment enables a user to perform business transactions from a user's computer 106 (PC or workstation) with those e-

- 11 -

Service providers 100, 102. The B2C environment, more particularly, includes a so-called "e-Company" 108 that offers a server instance 110 for handling these end-to-end business transactions between the user and the number of sales-entity or service providers 100; 102. The server instance 110, in the present embodiment, is implemented by a dedicated middleware arranged between an IP layer and a server layer (OSI model), as discussed in more detail hereinafter.

The user's computer 106 accesses the Internet 104 via an e-Network provider 112 (= Internet access provider) wherein the connection between the computer 106 and the e-Network 112, in the present embodiment, is based on a usual telephone connection using a Plain Old Telephone Service (POTS) 114, an Integrated Services Digital Network (ISDN) switching network, or the like.

During a first log-on by the user to the e-Network provider 112, a communication channel 116 to a Network-Access-Server (NAS) 118 of the e-Network provider 112 is established. The NAS 118 is connected to a database 120. The database 120 particularly stores user information for the customers of the e-Network provider 112 and thus can perform a user authentication procedure during log-on of the user. The e-Network provider 112 further holds a stock (pool) of available IP addresses A, B, C, D, etc. After successful user log-on, the user is assigned one of these IP addresses, in the present example address 'A'.

It is now assumed that the user holds a special subscription with the e-Network provider 112 for performing end-to-end business transactions, or even private end-to-end transactions with other Internet users, using the server instance 110 of

- 12 -

the invention. In that case, the provider 108 of the server instance (middleware) 110, in advance, provides a virtual private network (VPN) dialer to the user's computer 106 that can be used for those transactions. The VPN dialer enables to build up a virtual private network connection, in form of a point-to-point (PPP) connection, between the user's computer 106 and the server instance 110. Hereby, the user is assigned another IP address out of the pool of existing available IP addresses on side of the server instance 110. The pending VPN connection based on the new IP address 'b' is particularly implemented as an IP tunneling connection 122 between the user's computer 106 and the server instance 110, as indicated by the dotted line in Fig. 1.

A VPN, as known in the prior art, is a group of two or more computer systems, typically connected to a private network (a network built and maintained by an organization solely for its own use) with limited public-network access, that communicates "securely" over a public network. VPNs may exist between an individual machine and a private network (client-to-server) or a remote LAN and a private network (server-to-server). Security features differ from sales-entity (product) to sales-entity, but most security experts agree that VPNs include encryption, strong authentication of remote users or hosts, and mechanisms for hiding or masking information about the private network topology from potential attackers on the public network.

Now summarizing the principles of the embodiment illustrated in Fig. 1, the above described server instance 110 demands and insures single log-on for user authentication. A user log-on establishes a session context 124 between the user's currently assigned IP-address and his account. Any transaction with an

- 13 -

arbitrary e-Service provider 100, 102 will be authorized using the proposed server instance 110 during the lifetime of the session context 124. The authorization of any e-Service 100, 102 towards the server instance 110 will only require the clients IP-address, which is the most basic attribute in the Internet 104 as such.

More specific, an e-Service provider 100, 102 like an Internet shop integrated as proposed herein, would just have to use the user's IP-address to authenticate the user, by using a query service which is part of the proposed server instance 110 architecture. The user, in turn, may only use an alias within the e-Service provider 100, 102. The server instance 110, in turn, keeps track of any accounting events in terms of e.g. service identifier, number and price. This additionally allows for pre-billing and surveillance of prepaid accounts and/or budgeted accounts for basic billing requirements usually found in the area of micro-payments. The accounting records thus can be forwarded to a post billing instance. That post billing instance interfaces to an instance owning pricing plans.

The proposed server instance (middleware) 110 supports any number of e-companies which are defined as follows: They either offer a single service or a variety of services either owned by themselves or based on partnership agreements with others. The key requirement is, that these companies maintain and own contractual relationships to their subscribers, kept in a customer care or even self care system. The user attributes maintained here for each user and user sub account may be grouped as follows: Attributes relevant for User Account Authentication and Authorization, e.g. User ID, Account Number, Password, User-Alias..., full user address details, e.g. full address information, passport number etc.,

- 14 -

generic content related, e.g. filters, user preferences ..., payment related, e.g. from which bank account to collect micro payments or other payments. Further, in an environment of real goods, invoicing is triggered after customer delivery and customer acknowledgement. This will be achieved by introducing workflow components that will include mobile access techniques as well as parcel services. Again the already established real world rules will apply.

In addition, it is noteworthy that the server instance 110, due to the IP tunneling connection 122, can be physically located anywhere in the Internet 104, but preferably will be located inside the Firewalls of an Intranet of the e-Network provider 112, or the e-Company 108 likewise, if the e-Company 108 is a separate company from the e-Network provider 112. Further, the server instance 110, in the preferred embodiment, uses a Remote Authentication Dial In User Service (RADIUS) protocol, provided by a dedicated RADIUS server 126, discussed hereinafter.

It is emphasized that, in cases where the e-Network provider 112 is also providing the above described e-Company services 108 based on a server instance 110 in accordance with the invention, i.e. is keeping the server instance 110, it is not necessary to assign the above mentioned two IP addresses during log-on of the user since the middleware provider then will assign the IP address for authentication purposes.

Referring to Fig. 2, basic aspects concerning assignment of IP addresses according to the prior art are illustrated. Fig. 2 shows an example of two possible connection scenarios using the server instance (middleware) 200. A first computer 202 has

- 15 -

Internet 203 access using NAS-1 204, which belongs to a first e-network provider 206. The first e-network provider 206 is not using the middleware 200 to authenticate users and assign IP-addresses. The first e-network provider 206 has his own pool of IP addresses (e.g. 152.140.1.1/0) which are unknown to the middleware 200. The first computer 202 runs a tunneling client, which establishes a tunneling connection 208 to the middleware 200, allowing him to authenticate himself and receive a "middleware" IP-address (193.123.4.12). As described above and in the following in more detail, the middleware 200 creates a session context for the first computer 202 and maintains that session context until his sign-off. Having this IP-address, the first computer 202 can take advantage of all the features provided by the middleware 200 e.g. single sign-on.

A second computer 210 has also Internet 203 access using NAS-2 212, which belongs to a second e-network provider 214, using the middleware 200 too to authenticate and assign IP-addresses. The second e-network provider 214 also uses his own pool of IP-addresses (193.123.5.1/0), which are, in contrast to the first e-network provider 206, known/handled to/by the middleware 200. Because the Internet access of the second computer 210 via NAS-2 212 is controlled by the middleware 200, in this case, no tunneling connection is necessary to generate/maintain the necessary session-context.

Like the B2C scenario illustrated in Fig. 1, both computers 202, 210 can conduct business transactions with e-companies 216 and/or e-service providers 218, 220 using the middleware 200, regardless of if they received their "middleware" IP-address via a NAS or via a tunneling client, as described beforehand.

- 16 -

Referring now to Fig. 3, a preferred embodiment of the transaction process according to the invention by way of a process flow diagram is illustrated. Fig. 3 also shows the basic principles of how to establish a session context within an IP network and how to provide services and track all relevant accounting information and billing parameters based on dedicated service characteristics. In the diagram, the y direction, starting from the top, represents the time t, and the two vertical lines 300, 302 arranged in the x direction, represent to different transaction contexts, in the present example particularly to the pre-described session context and, in addition, one sales entity context (reference number '128' in Fig. 1).

The process begins with a sign-on procedure (step 'a') by the user which includes user authentication, as described beforehand. An IP address is assigned and a session context is created using the above mentioned RADIUS protocol. A session context records RADIUS-provided information like: Username, Framed-IP-Address and Class, Acct-Session-ID. The session context expires, when the user signs (logs) out or is disconnected.

Only during a pending session context, other transaction events initiated by the user or any e-Service provider being involved in a business transaction can principally occur wherein the session context is confirmed (step 'b'). The moment a user orders a sales-entity, an Authorization-Request is sent (step 'c') to the server instance (reference number '110' in Fig. 1). The middleware validates the user's sales-entity request and grants that the user is liable for these costs. A so called sales-entity context is generated (step

- 17 -

'c'). In the present example, the user requests a video-on-demand service from the e-Service provider. After his successful authorization (step 'c'), the start of the requested video-on-demand (VoD) service is indicated (step 'd') with an Accounting-Message (Acct-Start). When the VoD-service is finished, e. g. having downloaded or streamed the complete video file, an Accounting-Message (Acct-Stop) is generated in order to conduct the necessary billing for the downloaded video. The pending sales-entity context is deleted (step 'f').

When the user signs off, the recorded session context is deleted and the pending IP address de-allocated. Further an accounting-stop event is triggered (step 'g').

Any special service-event like rewind, pause/resume or forward the video during the streaming, will trigger an Accounting-Message (Acct-Intermediate).

The described session context is maintained by the proposed middleware. Any service layer will interface to the middleware in terms of service authorization and accounting.

It is emphasized that any security holes (viruses, worms or other attacks onto the client's computer) being existent throughout a pending online session comprising the above described session context can be resolved on side of the client's computer using known Firewall software solutions which effectively controls and monitors operating systems sockets. These security software solutions can be provided by an e-Company (in the above sense) as an e-Service (also in the above sense). In combination with the above described

- 18 -

communication protocol, particularly including the session context, the security level achieved hereby is much more higher than in prior art approaches.

In the following, referring to Fig. 4, the previously mentioned RADIUS (Remote Authentication Dial In User Service) protocol, published e.g. in RFC2865, RFC2866, RFC2867 and RFC2868 (www.ietf.org) is described in more detail.

The RADIUS protocol sets out a method of carrying out authentication, authorization and configuration information between a Network Access Server (NAS) 400 and a Shared Authentication Server. A first key feature of RADIUS is the underlying Client/Server Model where a Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers 402, and then acting on the response that is returned. In contrast to that, RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

It should be mentioned that communication between a NAS and a RADIUS server is based on the known User Datagram Protocol (UDP). UDP, documented in protocol standard RFC 768, provides users access to IP-like services. UDP packets are delivered just like IP packets - connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary. More particularly, UDP is defined to make available a datagram mode of packet-switched computer communication in the

- 19 -

environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol. UDP is mainly used in application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP).

The above mentioned authentication request message contains the user-supplied name and password, as well as the identity of the access device sending the request and the port being used for the remote connection. Since communication with the RADIUS server occurs across the network, the user-supplied password is typically encrypted by the NAS before the authentication request is sent to minimize the chance for compromise.

The authentication request can be sent to either a "local" RADIUS server via the local area network or to a "remote" server over a wide area network. This provides flexibility in designing the overall network architecture by allowing placement of the RADIUS server at the most appropriate location, not necessarily at the physical point of remote access. This is an important feature in cases where a "host" organization must maintain control of the authentication process but wishes to outsource most or all other elements of the remote access infrastructure. The RADIUS protocol also facilitates authentication redundancy by allowing the client devices to route requests to alternative servers if the primary RADIUS server cannot be reached.

- 20 -

When the RADIUS server receives the authentication request, it validates the request (to ensure it originated from a valid client device) and then decrypts the data packet to expose the user name and password. These credentials are then passed to the system being used to conduct the authentication process. The information used to authenticate the user sign-on (log-on) request can be contained in a password file, centralized authentication database, or a custom (or proprietary) system. Other commercial security systems (e.g., Kerberos) that support the RADIUS protocol can also be interfaced with to provide authentication.

If the credentials (name and password) of the user requesting access are properly matched against the stored information, the RADIUS server returns an authentication acknowledgement message to the NAS. This message contains the connection information (network type and services) necessary for attaching the authenticated user to the network. Hence, the type of connection (TCP/IP, PPP, SLIP, etc.) and access restrictions are applied to the user's login in accordance with pre-established policies. In the opposite case, if the credentials received from the RADIUS client do not match information in the authentication information store, the server returns an authentication reject message to the NAS. This message causes the NAS to deny access to the user requesting it.

In addition to the encryption of the user password during communications between the NAS and the authentication server, the RADIUS protocol also provides for additional security to avoid compromise of authentication via tampering with the message transfer process. As mentioned above, the messages passed between RADIUS clients and servers are validated to

- 21 -

prevent "spoofing" of these requests. The RADIUS server accomplishes this by sending an authentication key to the RADIUS client devices. This message acts as a digital signature to ensure that the proper authentication server is truly originating authentication messages.

The RADIUS protocol thus provides a high level of network security since transactions between the client and RADIUS server are authenticated through the use of a shared "secret", which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

In addition, RADIUS provides flexible authentication mechanisms since the RADIUS server can support a variety of methods to authenticate a user. It can support PPP PAP or CHAP, UNIX login, and other authentication mechanisms. Last but not least RADIUS is a highly extensible protocol since all transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol.

Concerning authentication and authorization, the RADIUS server 402 can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms. Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server 402 and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, encrypted password, NAS IP address, and additional information of the type of network connection.

- 22 -

When the RADIUS server 402 receives the Access-Request from the NAS, it searches a database for the username listed. If the username does not exist in the database, either a default profile is loaded or the RADIUS server 402 immediately sends an Access-Reject message. This Access-Reject message can be accompanied by a text message indicating the reason for the refusal.

The RADIUS accounting functions allow data to be sent at the start and end of sessions, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use RADIUS access control and accounting software to meet special security and billing needs.

Transactions between the client and RADIUS server 402 are authenticated through the use of a shared secret, which is never sent over the network. In addition, user passwords are sent encrypted between the client and RADIUS server 402 to eliminate the possibility that someone snooping on an insecure network could determine a user's password.

The information technology (IT) based process or service according to the invention, in terms of the (OSI) model, preferably is implemented beyond an IP layer as a server instance or middleware of a server, as being illustrated in Fig. 5. It can be seen from Fig. 5 that the process is based on an interaction scenario comprising four main components, an e-Network Provider 500 providing the basic network infrastructure and backbone for executing the underlying communication protocols, one or more e-Service Providers 502 which a (not shown) user is interested to do any kind of

- 23 -

commercial or even non-commercial business(es), an e-Company 504 for managing the entire process and a middleware 506 arranged on top of the network infrastructure for processing a so-called "session context" as described in more detail hereinafter and for providing AAA control facility and sales entity management for conducting the prementioned businesses in accordance with the novel business process according to the invention.

Fig. 5, for that purpose, depicts the general architectural structure of the proposed solution. In the present embodiment, the key point is that the middleware engine resides upon the IP network layer, provided by an e-Network Provider. This e-Network Provider can support several access method (like POTS, ISDN, Mobile, ...). The different components shown in Fig. 5 are

1. Network-Connector 508

When a client accesses the Middleware 506 via a network, which is not operated by the Middleware Provider, it is necessary to establish a session context with an IP-Address provided by the Middleware. This is done by the Network-Connector using VPN-Techniques like GRE, PPTP, L2F, L2TP or any other Tunneling-Protocol. This method ensures, that the client can be authenticated via the AAA Control-Facility, allowing him to take full advantage of the Middleware features without restricting his access to the (inter)net in any way.

If the e-Network Provider and the Middleware Provider happen to be the same company, there is no need for a VPN, because the AAA Control-Facility (2) of the middleware is the authentication authority for the network access as well, thus providing the client with a "Middleware" IP-Address.

2. AAA Control-Facility 510

- 24 -

The AAA Control-Facility is responsible for the authentication of the client providing an IP-Address after a successful verification of the user data against the user database of the corresponding e-Company. It keeps the client's session context until his logoff.

It authorizes the client, when he wants to consume or buy any sales entity provided by an e-Service provider. It compares authorization request against the user's profiles concerning service-subscription and personal information.

If the middleware provider happens to be the network provider of this client as well, it also maintains the user's access characteristics in an access profile, which also can be used for service authorization.

3. Sales-Entity Management 512

If a user/client wants to consume / buy a Sales-Entity, a context for this Sales-Entity is generated by the SE-Management. When a Sales-Entity is ordered, the e-Company asks SE Management to check if the cost of the Sales-Entity is covered in compliance with the customer's payment policy (prepaid account, credit line, credit card). The SE Management responds with a confirmation or a reject.

The SE Management keeps track of the different transactions and states during the whole buying process.

After the confirmation of the complete delivery of the Sales-Entity, an accounting event is generated and sent to the Billing component of the corresponding e-Company, the context then will be terminated.

The SE-Management uses techniques like Short Messaging Service, Interactive Voice Response, email, web-access for confirmation and notification of the different transactions during the lifecycle of the Sales-Entity context.

- 25 -

4. CRM 514

The CRM is used by the e-Company operator to maintain the customer User Database.

5. User Database 516

The User Database contains all information about the e-Company's customers (user-profile like payment policies, address, age, ...; service-profile like subscriptions).

6. Billing 518

The Billing component of the e-Company interfaces to the different credit card and banking institutes. It conducts the payments for the consumed / bought Sales-Entities according to the customers preconfigured payment policy.

The Billing component also does the invoicing and carries out the payments to the e-Service Provider.

7. e-Service-Connector 520

The e-Service-Connector integrates one or several e-Service Provider into a sales/marketing platform. It allows the e-Service Provider to offer his Sales-Entities through the e-Company, without having the need to acquire customer informations and concern billing modalities.

Fig. 6, shows a possible business-to-business (B2B) transaction environment, where the proposed middleware 600 inter-operates with three different e-companies 602 - 606 over the Internet 608. Each of these e-companies 602 - 606 holds a stock of users (customers), who can leverage the full advantage of all middleware 600 features. It is noteworthy that, in Fig. 6, the users, the NAS and the e-service

- 26 -

providers are omitted for simplification purposes only. Further, each e-company 602 - 606 maintains a corresponding user database 609, 610, 612 for these users and a RADIUS server 614 - 618 for conduction the above described AAA services.

Finally, in Fig. 7 possible integration profiles for the main components of the network layer structure shown in Fig. 5 are shown by way of an overview of all considered player roles. In theory there are some more possible combinations of the four main components, but they are of no practical meaning. In the following, the six shown Integration Profiles are described in more detail wherein referring to the numerals I) - VI) in Fig. 3.

I) A company, e.g. a Telco as a former classical network provider, which acts in all four layers (e-Network Provider, Middleware Operator, e-Company and e-Service Provider) is able to offer a multi-service ASP platform. In which the network operator with his business units also acts as an e-company by using his own infrastructure. He offers his own e-services and is able to integrate e-services from other service providers thus leveraging his large subscriber database. The Telco may as well offer real transaction based payment services to the integrated service providers (i.e. retailers).

II) Shows a company similar to the one that is described in I), which doesn't offer any e-Services of its own.

III) A Company that wants to host e-companies will act as e-network provider and middleware operator. It will offer access, delivery and secure, consumption-oriented payment and

- 27 -

workflow management services. The company profile number VI) shows a possible customer for this company.

IV) Shows a variation of the company example I) that doesn't own any network services itself.

V) Shows a company which offers hosting services described in II) but operates no network of its own and offers no e-services.

VI) Shows a company offering e-services of its own and hosting services for e-service provider.

- 28 -

C L A I M S

1. A method for handling end-to-end business transactions between a user and at least one sales-entity and/or service provider via a TCP/IP controlled computer network, wherein providing a transaction managing instance for managing said end-to-end business transactions, said method comprising the steps of:

providing a pool of IP addresses on side of said transaction managing instance;

performing an access authentication based single sign-on by said user managed by said transaction managing instance wherein said transaction managing instance is allocating an IP address out of said pool of IP addresses to said user, when the user initiates an online session for conducting at least one end-to-end business transaction with said at least one sales-entity and/or service provider;

generating a session context including at least said allocated IP address and user identification information;

transmitting an authorization request from the at least one sales-entity and/or service provider, or another service provider, to said transaction managing instance, when an at least one end-to-end business transaction with said at least one sales-entity and/or service provider occurs, wherein the transaction managing instance validates the user's authorization for said at least one business transaction based on said session context;

- 29 -

monitoring said online session of said user and detecting if said online session is terminated;

invalidating said allocated IP address and said session context, if termination of said online session is detected, and providing said IP address back to said pool of IP addresses.

2. Method according to claim 1, wherein providing an IP tunneling connection between the user and said transaction managing instance after said single sign-on.

3. Method according to claim 2, wherein said IP tunneling connection is a virtual private network (VPN) connection.

4. Method according to any of the preceding claims, wherein said session context is confirmed at least during a first accounting start event and wherein said session context is terminated by an accounting stop event.

5. Method according to claim 4, wherein said session context is used to perform accounting and/or authentication and/or authorization during an at least one end-to-end business transaction.

6. Method according to claim 4 or 5, wherein said session context particularly contains the username of said user and an accounting session identifier related to an accounting event.

7. Method according to any of claims 4 to 6, wherein said session context, in addition, contains a class attribute for the correlation of service-events.

- 30 -

8. Method according to any of the preceding claims, wherein recording or storing at least said IP address allocated to said user together with at least one attribute relevant for accounting and/or authentication and/or authorization.

9. Method according to claim 8, wherein closing said online session and said session context and removing the IP address and said at least one attribute from the record or storage if said user signs out or is disconnected from said transaction managing instance.

10. A data processing program for execution in a data processing system comprising software code portions for performing a method according to any of claims 1 to 9 when said program is run on said computer.

11. A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to any of claims 1 to 9 when said program is run on said computer.

12. A system for handling end-to-end business transactions between at least one user and at least one sales-entity and/or service provider via a TCP/IP controlled computer network, wherein said system includes a transaction managing instance for managing said end-to-end business transactions and wherein said transaction managing instance comprises:

a pool of IP addresses available for allocation to the at least one user;

means for performing an access authentication based single sign-on by said at least one user and for allocating an IP

- 31 -

address out of said pool of IP addresses to said at least one user;

means for generating a session context including at least said allocated IP address and user identification information;

means for processing an authorization request transmitted from the at least one sales-entity and/or service provider, or another service provider, when an at least one end-to-end business transaction with said at least one sales-entity and/or service provider occurs, and for validating the user's authorization for said at least one business transaction based on said session context;

means for monitoring said online session of the at least one user and for detecting if said online session is terminated;

means for invalidating said allocated IP address and said generated session context, if termination of said online session is detected, and for providing said IP address back to said pool of IP addresses.

13. System according to claim 12, further comprising means for establishing an IP tunneling connection between the at least one user and said transaction managing instance after said single sign-on.

14. System according to claim 13, wherein said IP tunneling connection is a virtual private network (VPN) connection.

15. System according to any of claims 12 to 14, wherein said session context particularly contains the username of said at least one user and an accounting session identifier related to an accounting event.

- 32 -

16. System according to claim 15, wherein said session context, in addition, contains a class attribute for the correlation of service-events.

17. System according to any of claims 12 to 16, comprising means for recording or storing at least said IP address allocated to said user together with at least one attribute relevant for accounting and/or authentication and/or authorization.

18. System according to claim 17, further comprising means for closing said online session and said session context and for removing the allocated IP address and said at least one attribute from said record or storage if said at least one user signs out or is disconnected from said transaction managing instance.

1 / 6

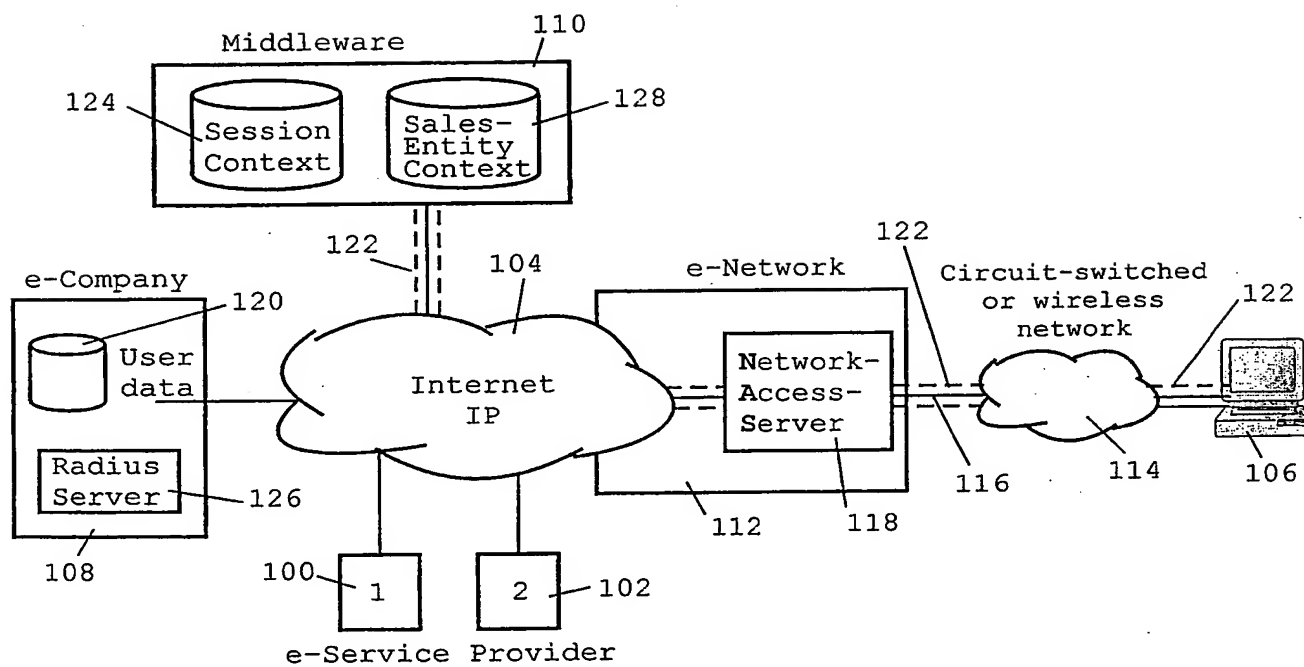


FIG. 1

2 / 6

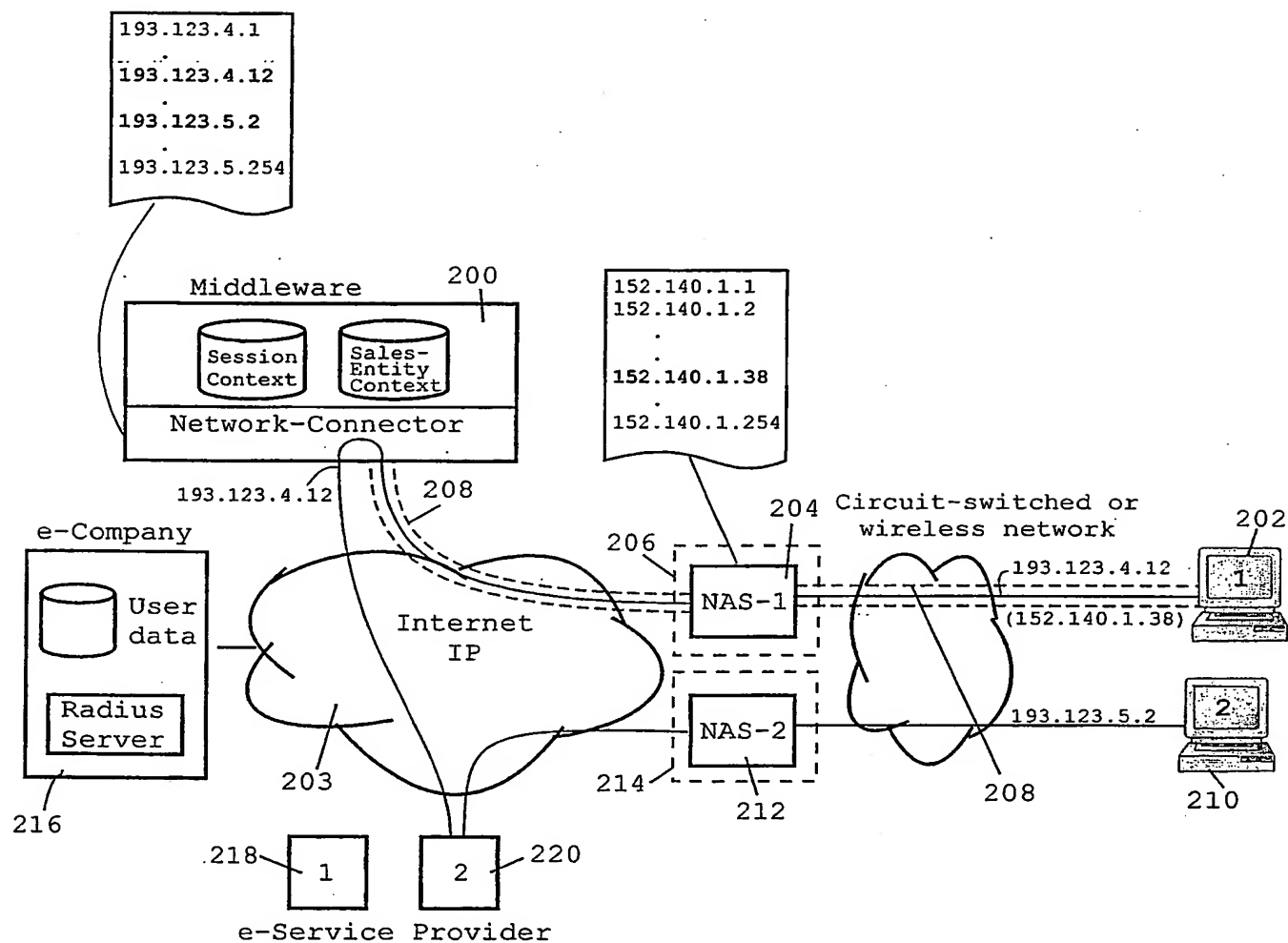


FIG. 2

3 / 6

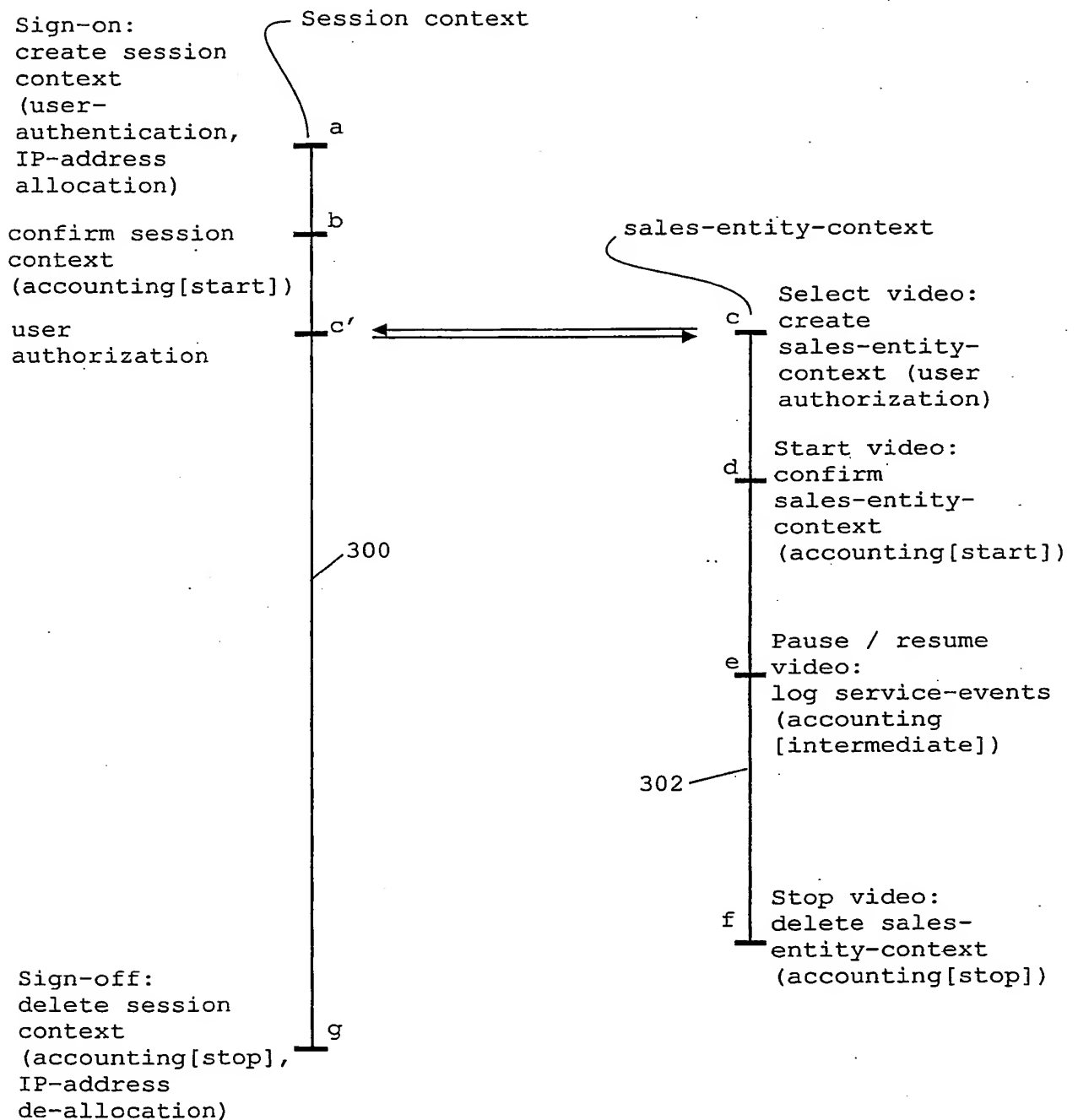


FIG. 3

4 / 6

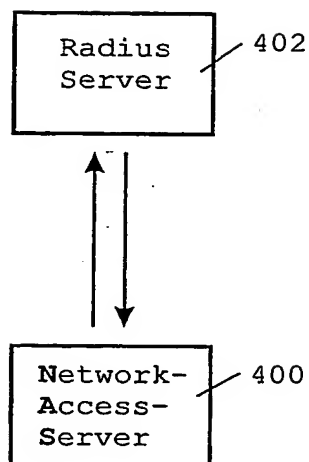


FIG. 4

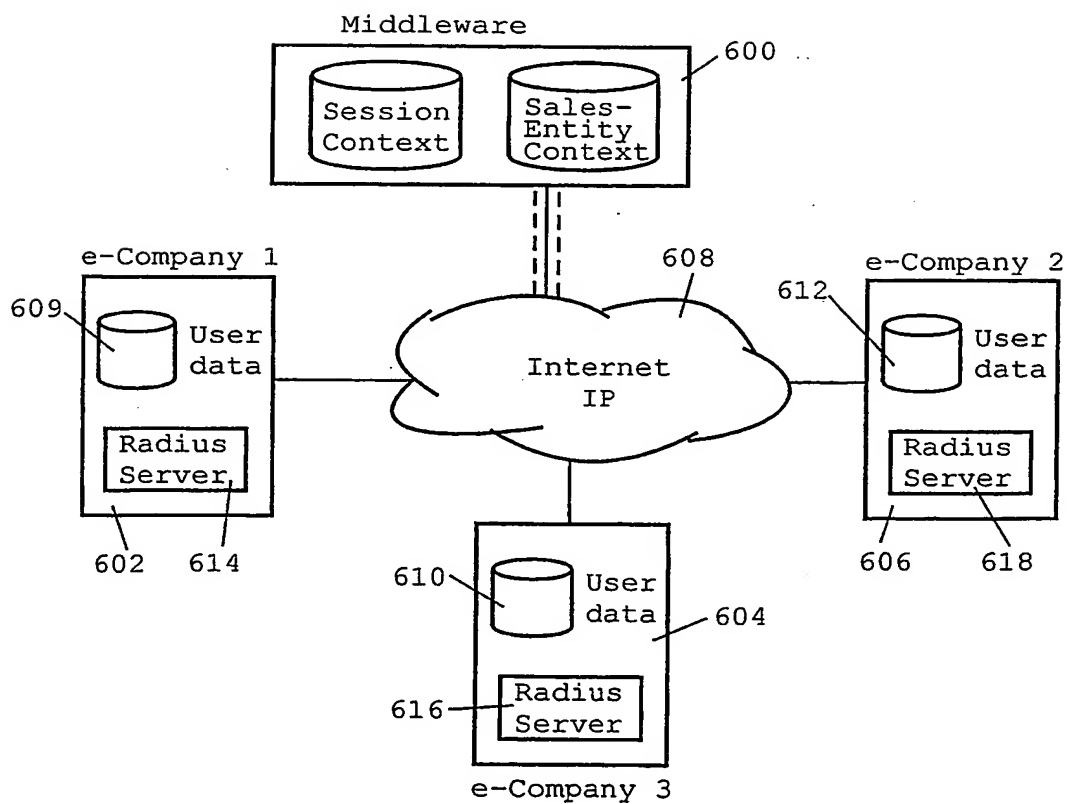


FIG. 6

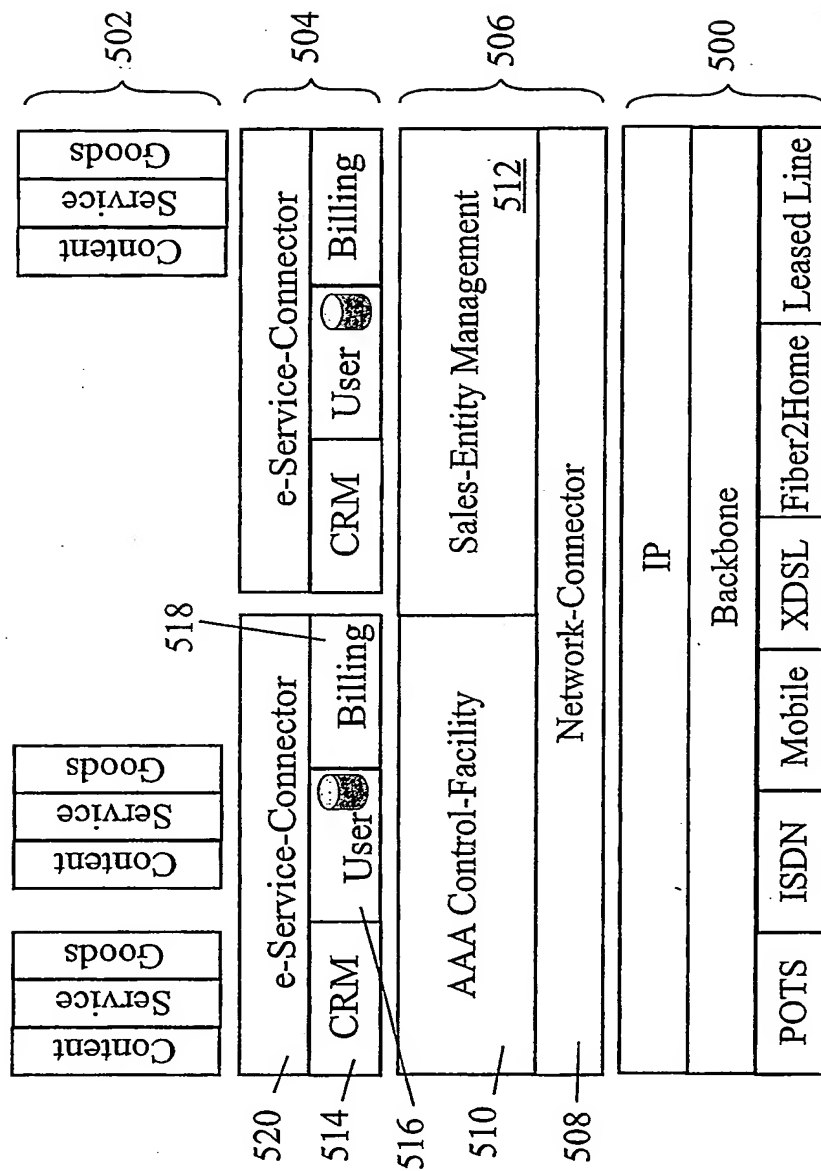


FIG. 5

Integration profiles					
I	II	III	IV	V	VI
e-Service Provider ★ Content ★ Service ★ Goods			e-Service Provider ★ Content ★ Service ★ Goods		e-Service Provider ★ Content ★ Service ★ Goods
e-Company ★ Any company's business unit(s) ★ User (subscriber, employee, company, device) ★ Inter company	e-Company ★ Any company's business unit(s) ★ User (subscriber, employee, company, device) ★ Inter company		e-Company ★ Any company's business unit(s) ★ User (subscriber, employee, company, device) ★ Inter company	e-Company ★ Any company's business unit(s) ★ User (subscriber, employee, company, device) ★ Inter company	e-Company ★ Any company's business unit(s) ★ User (subscriber, employee, company, device) ★ Inter company
Middleware ★ Session context ★ Workflow component ★ Peering component	Middleware ★ Session context ★ Workflow component ★ Peering component	Middleware ★ Session context ★ Workflow component ★ Peering component	Middleware ★ Session context ★ Workflow component ★ Peering component	Middleware ★ Session context ★ Workflow component ★ Peering component	
e-Network Provider ★ Remote access ★ Backbone ★ NOC	e-Network Provider ★ Remote access ★ Backbone ★ NOC	e-Network Provider ★ Remote access ★ Backbone ★ NOC			

FIG. 7

INTERNATIONAL SEARCH REPORT

Internati Application No
PCT/Er 02/13493

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 845 070 A (IKUDOME KOICHIRO) 1 December 1998 (1998-12-01) the whole document ---	1-18
A	US 6 032 260 A (SCHNEIDER DAVID H ET AL) 29 February 2000 (2000-02-29) column 6, line 65 -column 10, line 63 ---	1-18
A	US 6 311 275 B1 (CHU JIE ET AL) 30 October 2001 (2001-10-30) column 3, line 50 -column 5, line 60 -----	1-18

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

2 June 2003

Date of mailing of the international search report

11/06/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Beatty, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/L. 02/13493

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5845070	A	01-12-1998	NONE	
US 6032260	A	29-02-2000	NONE	
US 6311275	B1	30-10-2001	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.